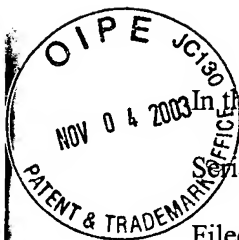


4777-31

11-06-03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In the application of: Hisashi TAKAYAMA & Junko FURUYAMA

Serial No.: 10/647640

Filed: August 25, 2003

For: **Authentication Method, System and Apparatus of an Electronic Value**

Assistant Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy(ies) of three foreign applications from which priority is claimed for this case.

1)Country: Japan

Application No.: 2003-289433

Filing Date: August 7, 2003

2)Country: Japan

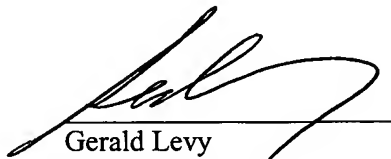
Application No.: 2003-072284

Filing Date: March 17, 2003

3)Country: Japan

Application No.: 2002-245997

Filing Date: August 26, 2002


Gerald Levy
Registration No. 24,419

Date: November 4, 2003

MAILING ADDRESS

Pitney, Hardin, Kipp & Szuch LLP
685 Third Avenue
New York, New York 10017-4024
(212) 297-5800

I hereby certify that this paper is being deposited on November 4, 2003 with the U.S. Postal Service as First Class Mail, addressed to: Assistant Commissioner for Patents, Alexandria, VA 22313-1450


Gerald Levy

November 4, 2003
Date

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Account No. 50-1145, Order.

EV167248154US

()

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 8 月 2 6 日
Date of Application:

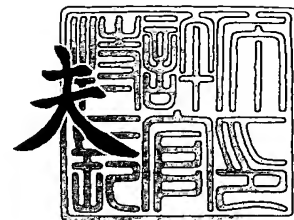
出 願 番 号 特 願 2 0 0 2 - 2 4 5 9 9 7
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 2 4 5 9 9 7]

出 願 人 松下電器産業株式会社
Applicant(s):

2 0 0 3 年 9 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 7 2 4 7 3

【書類名】 特許願

【整理番号】 2030744024

【提出日】 平成14年 8月26日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00
G06F 17/60

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地
松下電器産業株式会社内

【氏名】 高山 久

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地
松下電器産業株式会社内

【氏名】 古山 純子

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100082692

【弁理士】

【氏名又は名称】 蔵合 正博

【電話番号】 03-5210-2681

【選任した代理人】

【識別番号】 100081514

【弁理士】

【氏名又は名称】 酒井 一

【電話番号】 03-5210-2681

【手数料の表示】**【予納台帳番号】** 013549**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【包括委任状番号】** 0016258**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 電子バリュウの認証方式と認証システムと装置

【特許請求の範囲】

【請求項 1】 ユーザは暗号化された電子バリュウ(Encrypt(ev))・を保有し、前記電子バリュウ(ev)には、ユーザが指定した電子バリュウに対する認証情報(VPW)・を第 1 の不可逆演算処理(F)したバリュウ認証情報(F(VPW))が含まれており、ユーザが前記電子バリュウの正しい所有者であることを認証する処理において、認証側が乱数Rを生成してユーザ側に送信し、ユーザ側がユーザが入力した電子バリュウに対する認証情報(VPW')からバリュウ認証情報(F(VPW'))を生成し、更に、前記乱数Rと組み合わせたデータに第 2 の不可逆演算処理(G)を行い認証情報(G(R, F(VPW'))))を生成して、前記暗号化された電子バリュウと共に認証側に送信し、認証側が受信した暗号化された電子バリュウの暗号を復号化して、電子バリュウからバリュウ認証情報(F(VPW))を取り出し、前記乱数Rと組み合わせたデータに第 2 の不可逆演算処理(G)を行い認証情報(G(R, F(VPW)))を生成し、前記受信した認証情報(G(R, F(VPW'))))と認証情報(G(R, F(VPW)))とが一致することを検証して、ユーザを認証することを特徴とする認証方式。

【請求項 2】 前記暗号化された電子バリュウの暗号の復号化鍵は、バリュウ認証情報(F(VPW))を第 3 の不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリュウの正しい所有者であることを認証する処理において、ユーザ側が更にバリュウ認証情報(F(VPW'))を第 3 の不可逆演算処理(H)したデータ(H(F(VPW'))))を生成して、認証情報(G(R, F(VPW'))))と暗号化された電子バリュウと共に認証側に送信し、認証側が受信したデータ(H(F(VPW'))))とマスター鍵とから復号化鍵を生成して、受信した暗号化された電子バリュウの暗号を復号化することを特徴とする請求項 1 記載の認証方式。

【請求項 3】 前記電子バリュウには、電子バリュウの発行者による電子署名が施されており、ユーザが前記電子バリュウの正しい所有者であることを認証する処理において、認証側が暗号を復号化した電子バリュウに施された電子署名を検証することを特徴とする請求項 1 記載または請求項 2 記載の認証方式。

【請求項 4】 前記認証情報が、パスワードであることを特徴とする請求項 1

記載から請求項 3 のいずれかに記載の認証方式。

【請求項 5】 前記認証情報が、指紋や虹彩などの生体認証情報であることを特徴とする請求項 1 記載から請求項 3 のいずれかに記載の認証方式。

【請求項 6】 ユーザの携帯端末に暗号化された電子バリュー(Encrypt(ev))を格納し、前記電子バリュー(ev)には、ユーザが指定した電子バリューに対する認証情報(VPW)を第 1 の不可逆演算処理(F)したバリュー認証情報(F(VPW))が含まれており、ユーザが前記電子バリューの正しい所有者であることを認証する処理において、認証装置が乱数Rを生成して携帯端末に送信し、携帯端末がユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、前記乱数Rと組み合わせたデータに第 2 の不可逆演算処理(G)を行い認証情報(G(R, F(VPW'))))を生成して、前記暗号化された電子バリューと共に前記認証装置に送信し、認証装置が受信した暗号化された電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、前記乱数Rと組み合わせたデータに第 2 の不可逆演算処理(G)を行い認証情報(G(R, F(VPW)))を生成し、前記受信した認証情報(G(R, F(VPW'))))と認証情報(G(R, F(VPW)))とが一致することを検証して、ユーザを認証することを特徴とする認証システム。

【請求項 7】 前記暗号化された電子バリューの暗号の復号化鍵は、バリュー認証情報(F(VPW))を第 3 の不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリューの正しい所有者であることを認証する処理において、携帯端末が更にバリュー認証情報(F(VPW'))を第 3 の不可逆演算処理(H)したデータ(H(F(VPW'))))を生成して、認証情報(G(R, F(VPW'))))と暗号化された電子バリューと共に認証装置に送信し、認証装置が受信したデータ(H(F(VPW'))))とマスター鍵とから復号化鍵を生成して、受信した暗号化された電子バリューの暗号を復号化することを特徴とする請求項 6 記載の認証システム。

【請求項 8】 前記電子バリューには、電子バリューの発行者による電子署名が施されており、ユーザが前記電子バリューの正しい所有者であることを認証する処理において、認証装置が暗号を復号化した電子バリューに施された電子署名

を検証することを特徴とする請求項 6 記載または請求項 7 記載の認証システム。

【請求項 9】 前記携帯端末に格納された暗号化された電子バリューは、携帯端末からの電子バリュー発行要求に基づいて電子バリュー発行サーバが生成し、携帯端末にダウンロードされたものであり、前記電子バリュー発行要求には、ユーザが指定した電子バリューに対する認証情報(VPW)を第 1 の不可逆演算処理(F)したバリュー認証情報(F(VPW))が含まれ、前記電子バリュー発行サーバがバリュー認証情報(F(VPW))を用いて暗号化された電子バリューを生成することを特徴とする請求項 6 から請求項 8 のいずれかに記載の認証システム。

【請求項 1 0】 前記電子バリューが、電子情報化された会員証、または、電子情報化された I D カードであることであることを特徴とする請求項 6 から請求項 9 のいずれかに記載の認証システム。

【請求項 1 1】 前記電子バリューが、電子情報化されたクレジットカード、または、電子情報化されたデビットカードであることであることを特徴とする請求項 6 から請求項 9 のいずれかに記載の認証システム。

【請求項 1 2】 前記電子バリューが、電子情報化されたチケット、または、電子情報化されたクーポンであることであることを特徴とする請求項 6 から請求項 9 のいずれかに記載の認証システム。

【請求項 1 3】 前記認証情報が、パスワードであることを特徴とする請求項 6 記載から請求項 1 2 のいずれかに記載の認証システム。

【請求項 1 4】 前記認証情報が、指紋や虹彩などの生体認証情報であることを特徴とする請求項 6 記載から請求項 1 2 のいずれかに記載の認証システム。

【請求項 1 5】 携帯端末からの電子バリュー発行要求に基づいて、バリュー認証情報(F(VPW))を電子バリューの中に入れ、暗号化された電子バリューを生成して、携帯端末に送信することを特徴とする電子バリュー発行サーバ。

【請求項 1 6】 ユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、認証装置から乱数Rと組み合わせたデータに第 2 の不可逆演算処理(G)を行い認証情報(G(R, F(VPW'))))を生成して、暗号化された電子バリューと共に認証装置に送信することで、ユーザが電子バリューの正しい所有者であることの認証を受けることを特徴とする携帯端末。

【請求項 17】 生態認証手段を具備し、前記認証情報が、前記生態認証手段から入力される指紋や虹彩などの生態認証情報であることを特徴とする請求項 16 記載の認証システム。

【請求項 18】 乱数Rを生成して携帯端末に送信し、携帯端末から受信した認証情報($G(R, F(VPW'))$)と暗号化された電子バリューとから、暗号化された電子バリューの暗号を復号化して、電子バリューからバリュー認証情報($F(VPW)$)を取り出し、前記乱数Rと組み合わせたデータに第2の不可逆演算処理(G)を行い認証情報($G(R, F(VPW))$)を生成し、受信した認証情報($G(R, F(VPW'))$)と認証情報($G(R, F(VPW))$)とが一致することを検証して、ユーザを認証することを特徴とする認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、クレジットカードやデビットカード、会員証、IDカード、チケットなどを電子情報化した電子バリューをユーザの携帯端末に格納し、ユーザが、それらの正しい所有者であることを認証することで、それぞれに対応する物やサービスがユーザが提供されるサービスにおいて、携帯端末が耐タンパ機能のない端末であっても、安全なユーザ認証処理を可能にするものである。

【0002】

【従来の技術】

従来の技術では、安全な認証処理を行うために耐タンパ機能を備えたICカードモジュールを携帯電話に搭載し、そのICカードモジュールには、予め、公開鍵暗号方式のプライベート鍵と公開鍵の鍵ペアが格納され、例えば、クレジットカードの場合には、その公開鍵を用いたクレジットカードの証明書を携帯電話に格納し、クレジットカードの利用時には、携帯電話がプライベート鍵を用いて電子署名処理を行い、認証側ではその電子署名をクレジットカードの証明書をを用いて検証することで、ユーザ認証が行われていた。

【0003】

【発明が解決しようとする課題】

しかし、従来の技術では、携帯電話または携帯端末に耐タンパ機能を備えた IC カードモジュールを搭載する必要があり、端末のコストがアップある課題があった。

【0004】

本発明は、こうした従来の問題点を解決するものであり、耐タンパ機能のない携帯端末であっても、安全な認証処理が出来る認証方式、及び、認証システムを提供し、また、そのシステムを実現する装置を提供することを目的としている。

【0005】

【課題を解決するための手段】

そこで、上記の目標を達成するため、本発明の認証方式では、ユーザは暗号化された電子バリュー(Encrypt(ev))を保有し、電子バリュー(ev)には、ユーザが指定した電子バリューに対する認証情報(VPW)・を第1の不可逆演算処理(F)したバリュー認証情報(F(VPW))が含まれており、ユーザが前記電子バリューの正しい所有者であることを認証する処理において、認証側が乱数Rを生成してユーザ側に送信し、ユーザ側がユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報(F(VPW'))を生成し、更に、乱数Rと組み合わせたデータに第2の不可逆演算処理(G)を行い認証情報(G(R, F(VPW'))))を生成して、暗号化された電子バリューと共に認証側に送信し、認証側が受信した暗号化された電子バリューの暗号を復号化して、電子バリューからバリュー認証情報(F(VPW))を取り出し、乱数Rと組み合わせたデータに第2の不可逆演算処理(G)を行い認証情報(G(R, F(VPW)))を生成し、受信した認証情報(G(R, F(VPW'))))と認証情報(G(R, F(VPW)))とが一致することを検証して、ユーザを認証する。本認証方式によれば、ユーザ側に暗号鍵等の秘密情報を格納する必要がなく、耐タンパ機能も必要ないが、認証側では安全にユーザを認証することができる。

【0006】

また、さらに、本発明の認証方式では、暗号化された電子バリューの暗号の復号化鍵は、バリュー認証情報(F(VPW))を第3の不可逆演算処理(H)・したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリューの正しい所有者であることを認証する処理において、ユーザ側が更にバリュー認証

情報($F(VPW')$)を第3の不可逆演算処理(H)したデータ($H(F(VPW'))$)を生成して、認証情報($G(R, F(VPW'))$)と暗号化された電子バリューと共に認証側に送信し、認証側が受信したデータ($H(F(VPW'))$)とマスター鍵とから復号化鍵を生成して、受信した暗号化された電子バリューの暗号を復号化する。本認証方式によれば、電子バリュー毎に電子バリューを暗号化している暗号鍵が異なるため、仮に、一つの電子バリューの暗号が解かれたとしても、他の電子バリューには影響を与えないので、安全性を高めることができる。

【0007】

また、さらに、本発明の認証方式では、電子バリューには、電子バリューの発行者による電子署名が施されており、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、認証側が暗号を復号化した電子バリューに施された電子署名を検証する。本認証方式によれば、電子バリューの偽造を防止することができ、さらに、認証処理の安全性を高めることができる。

【0008】

また、本発明の認証システムでは、ユーザの携帯端末に暗号化された電子バリュー($Encrypt(ev)$)を格納し、前記電子バリュー(ev)には、ユーザが指定した電子バリューに対する認証情報(VPW)を第1の不可逆演算処理(F)したバリュー認証情報($F(VPW)$)が含まれており、ユーザが前記電子バリューの正しい保有者であることを認証する処理において、認証装置が乱数 R を生成して携帯端末に送信し、携帯端末がユーザが入力した電子バリューに対する認証情報(VPW')からバリュー認証情報($F(VPW')$)を生成し、更に、乱数 R と組み合わせたデータに第2の不可逆演算処理(G)を行い認証情報($G(R, F(VPW'))$)を生成して、暗号化された電子バリューと共に前記認証装置に送信し、認証装置が受信した暗号化された電子バリューの暗号を復号化して、電子バリューからバリュー認証情報($F(VPW)$)を取り出し、乱数 R と組み合わせたデータに第2の不可逆演算処理(G)を行い認証情報($G(R, F(VPW'))$)を生成し、受信した認証情報($G(R, F(VPW'))$)と認証情報($G(R, F(VP \cdot W))$)

とが一致することを検証して、ユーザを認証する。本認証システムによれば、携帯端末に暗号鍵等の秘密情報を格納する必要がなく、耐タンパ機能を搭載する必要がないが、認証装置では安全にユーザを認証することができる。

【0009】

また、さらに、本発明の認証システムでは、前記暗号化された電子バリューの暗号の復号化鍵は、バリュー認証情報(F(VPW))を第3の不可逆演算処理(H)したデータ(H(F(VPW)))とマスター鍵とから生成した鍵であり、ユーザが前記電子バリューの正しい所有者であることを認証する処理において、携帯端末が更にバリュー認証情報(F(VPW'))を第3の不可逆演算処理(H)したデータ(H(F(VPW'))))を生成して、認証情報(G(R, F(VPW'))))と暗号化された電子バリューと共に認証装置に送信し、認証装置が受信したデータ(H(F(VPW'))))とマスター鍵とから復号化鍵を生成して、受信した暗号化された電子バリューの暗号を復号化する。本認証システムによれば、電子バリュー毎に電子バリューを暗号化している暗号鍵が異なるため、仮に、一つの電子バリューの暗号が解かれたとしても、他の電子バリューには影響を与えないので、安全性を高めることが出来る。

【0010】

また、さらに、本発明の認証システムでは、電子バリューには、電子バリューの発行者による電子署名が施されており、ユーザが前記電子バリューの正しい所有者であることを認証する処理において、認証装置が暗号を復号化した電子バリューに施された電子署名を検証する。本認証システムによれば、電子バリューの偽造を防止することができ、さらに、認証処理の安全性を高めることができる。

【0011】

また、さらに、本発明の認証システムでは、携帯端末に格納された暗号化された電子バリューは、携帯端末からの電子バリュー発行要求に基づいて電子バリュー発行サーバが生成し、携帯端末にダウンロードされたものであり、電子バリュー発行要求には、ユーザが指定した電子バリューに対する認証情報(VPW)を第1の不可逆演算処理(F)したバリュー認証情報(F(VPW))が含まれ、前記電子バリュー発行サーバがバリュー認証情報(F(VPW))を用いて暗号化された電子バリューを生成する。本認証システムによれば、携帯端末に対して、各種の電子バリューを発行するサービスを行うことが出来る。

【0012】**【発明の実施の形態】**

本発明の実施形態の1つとして、電子クレジット決済システムについて説明する。

【0013】

電子クレジット決済システムは、ユーザが所有する携帯電話1とクレジットカード会社のセンター2と、小売販売店に設置されるクレジット決済端末3とによって構成され、携帯電話1とセンター2とは、携帯電話の無線通信ネットワークによって接続され、クレジット決済端末3とセンター2とはクレジット決済ネットワークによって接続され、携帯電話1とクレジット決済端末3とは、ローカルワイヤレス通信機能（赤外線通信、Bluetooth、無線LAN、非接触ICカードの無線通信など）を用いて、アドホックに通信する。携帯電話1には、予め、Javaクレジット決済アプリがダウンロードされている。また、クレジット決済端末3には、電子クレジットに施されたクレジットカード会社による電子署名を検証するため、クレジットカード会社の証明書が格納され、センター2とクレジット決済端末3には、電子クレジットの暗号鍵のマスター鍵 K_m が管理されている。携帯電話1には、ユーザが所有するクレジットカードに対応する電子クレジット（電子情報化したクレジットカード、電子バリューの一種）をセンター2からダウンロードする。

【0014】

図1は、電子クレジットのダウンロードの手順を示している。まず、ユーザがJavaクレジット決済アプリを起動(100)すると、メニュー画面が表示され(101)、ユーザが電子クレジット発行要求操作(102)を行うと、クレジットカードのカード番号とPIN、さらに、ダウンロードする電子クレジットに対応するパスワード(VPW)を入力する画面が表示される(103)。ユーザがカード番号とPIN、及び、パスワードを入力すると(104)、携帯電話1は、パスワード(VPW)のハッシュ演算結果 Hash(VPW)をパスワードの参照データとして携帯電話1のメモリに格納し(105)、さらに、カード番号(CN)と時刻(T)とから、ユーザ識別情報 $UID = Hash(CN || T)$ （※ || はデータの連結を示す）を生成してメモリに格納し(106)、さらに、パスワード(VPW)とユーザ識別情報(UID)とから、バリュー認証情報 $F(VPW) = Hash(VPW || UID)$ を生成し(107)、カード番号とPINとバリュ

一認証情報 F(VPW)とを含む、電子クレジット発行要求をセンター 2 に送信する (108)。

【0 0 1 5】

センター 2 は、カード番号と P I N とから、クレジットカードの所有者であるかユーザを認証し (109)、認証された場合に、電子クレジットの中にバリュー認証情報 F(VPW)を埋め込んで電子クレジット(ev)を生成する (110)。さらに、バリュー認証情報 F(VPW)のハッシュ演算し、マスター鍵 Km と連結して、さらに、ハッシュ演算して、電子クレジット(ev)を暗号化する共通鍵暗号方式の暗号鍵 $K_c = \text{Hash}(K_m \parallel \text{Hash}(F(VPW)))$ を生成する (111)。生成した暗号鍵 K_c を用いて、電子クレジット(ev)を暗号化して、暗号化された電子クレジット $\text{encrypt}(ev) = \text{Enc}(K_c, ev)$ を生成する (112)。暗号化された電子クレジット $\text{encrypt}(ev)$ は、携帯電話 1 に送信され (113)、暗号化された電子クレジット $\text{encrypt}(ev)$ は、携帯電話のメモリに格納され (114)、携帯電話 1 がダウンロードの完了を表示して、電子クレジットのダウンロード処理を完了する。

【0 0 1 6】

暗号化された電子クレジット 300 のデータ構造は、図 3 に示すようになっており、暗号化される前の電子クレジットは、クレジットカードのカード番号、有効期限、ユーザ名、発行者名等を示す電子クレジット情報 301 と、電子クレジット情報 301 の部分に対するクレジットカード会社による電子署名 302 と、バリュー認証情報 F(VPW) 303 とから構成されている。

【0 0 1 7】

J a v a クレジット決済アプリを終了すると、ユーザが入力したパスワードはメモリから消去される。携帯電話のメモリに保持されているデータは、パスワードをハッシュ演算したものであるため、仮に、携帯電話が第三者に盗まれて、内部のメモリが解析されたとしても、パスワードが知られる心配が無い。

【0 0 1 8】

次に、ダウンロードした電子クレジットを用いて、クレジットカード決済を行う手順について、図 2 を用いて説明する。

【0 0 1 9】

クレジット決済端末3がチャレンジ情報として乱数Rを生成する。ユーザがJavaクレジット決済アプリを起動(201)すると、メニュー画面が表示され(202)、ユーザが電子クレジット決済操作(203)を行うと、電子クレジットに対応するパスワード(VPW)を入力する画面が表示される(204)。ユーザがパスワード(VPW')を入力すると(205)、携帯電話1は、パスワード(VPW')のハッシュHash(VPW')を計算し、メモリに格納された参照データのHash(VPW)と照合してユーザを認証する(206)。参照データと一致しなかった場合にはエラーを表示し(図には記載していない)、参照データと一致した場合には、クレジット決済端末3からの電子クレジット要求を受信する(207)。電子クレジット要求には、乱数Rが含まれており、携帯電話1は、ユーザが入力したパスワード(VPW')を用いて、バリュース認証情報 $F(VPW') = \text{Hash}(VPW' || \text{UID})$ 及び、パスワードと乱数Rとの連結のハッシュ $\text{Hash}(F(VPW') || R)$ 、バリュース認証情報のハッシュ $\text{Hash}(F(VPW'))$ をそれぞれ計算し(208)、クレジット決済端末2に電子クレジットとして、暗号化された電子クレジット $\text{encrypt}(ev)$ と共に、 $\text{Hash}(F(VPW') || R)$ と、 $\text{Hash}(F(VPW'))$ とを送信する(209)。

【0020】

クレジット決済端末3は、受信したバリュース認証情報のハッシュ $\text{Hash}(F(VPW'))$ とマスター鍵 K_m とから、その連結のHashを計算し、暗号化された電子クレジットの共通鍵暗号方式の復号鍵 $K_c' = \text{Hash}(K_m || \text{Hash}(F(VPW')))$ を生成し、電子クレジットの暗号を復号化する(210)。クレジット決済端末3は、復号化した電子クレジット(ev)からクレジット認証情報F(VPW)を取り出し、乱数Rとの連結のハッシュ $\text{Hash}(F(VPW) || R)$ を計算し、携帯電話1から受信した $\text{Hash}(F(VPW') || R)$ と照合し、一致していた場合、ユーザが電子クレジットの正しい所有者であると認証する(211)。一致しなかった場合には、ユーザに対して、エラーを示す(図には記載してない)。さらに、クレジット決済端末3は、電子署名302を検証し(212)、エラーが検出された場合には、ユーザに対して、エラーを示す。電子署名302の検証(212)において、エラーが検出されなかった場合には、クレジット決済端末3は、携帯電話1に認証結果を送信し(213)、さらに、センター2にクレジット決済の承認要求を送信し(215)、センター2が承認処理を行い(21

6)、センター2からクレジット決済端末3に承認要求応答が送信されて(217)、クレジット決済端末3でのクレジット決済処理は完了する。

【0021】

一方、認証結果を受信した携帯電話1は、完了を表示して(214)、電子クレジットのクレジット決済処理を完了する。この場合も、Javaクレジット決済アプリを終了すると、ユーザが入力したパスワードはメモリから消去される。携帯電話1とクレジット決済端末3との間で交換されるデータは、すべて、ハッシュ演算、または、暗号化されたデータであるため、仮に、第三者が携帯電話1とクレジット決済端末3との間の通信が盗聴されたとしても、その盗聴したデータを用いて、成りすましを行うことは出来ない。

【0022】

また、以上では、電子クレジットに対応する認証情報をパスワードとしたが、ユーザの指紋や虹彩などの生体情報としても良い。この場合、携帯電話1は、指紋認証センサーや虹彩認証カメラなどの機能を備える。

【0023】

なお、本実施の形態では、電子クレジット決済システムについて述べたが、電子クレジットの電子クレジット情報301の部分の内容を変更することで、同様の認証メカニズムを電子デビット決済システムや、電子チケットシステム、電子クーポンシステム、または、会員証やIDカードなど、他の電子バリューの認証処理にも用いることができる。例えば、電子デビット決済システムの場合には、電子クレジット情報301の部分に、銀行口座番号、ユーザ名、発行者名などの情報を入れるがけでよい。

【0024】

【発明の効果】

以上の説明から明らかなように、本発明のデジタル鍵システム及びそれを構成する装置は、物理的な鍵を用いないため、ローコストで新たな鍵の生成ができる。また、鍵が紛失したときの対応が容易である。利用者は、鍵の受け渡したために特定の場所に赴く必要がなく、利便性が高い。

【0025】

また、鍵の利用に関する費用を精算するために電子決済を利用することが可能であり、提供するサービスに対する代金回収コストを低く抑えられる。

【 0 0 2 6 】

また、譲渡が可能であり、デジタル鍵を第三者にオンライン転送することができる。

【図面の簡単な説明】

【図 1】

本発明の実施形態における電子クレジットのダウンロード処理のフロー図

【図 2】

本発明の実施形態における電子クレジットの使用処理のフロー図

【図 3】

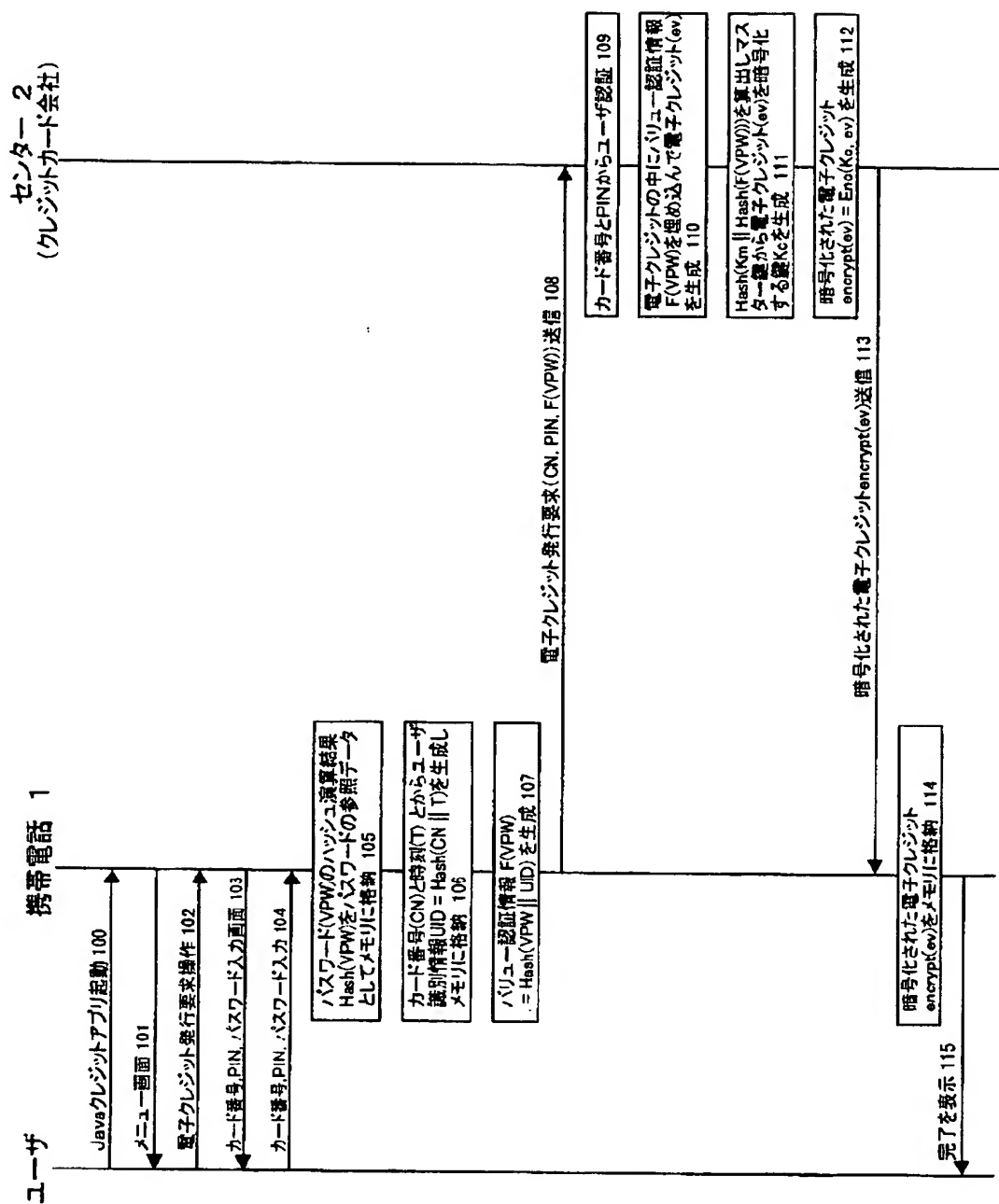
本発明の実施形態における電子クレジットのデータ構造を示す模式図

【符号の説明】

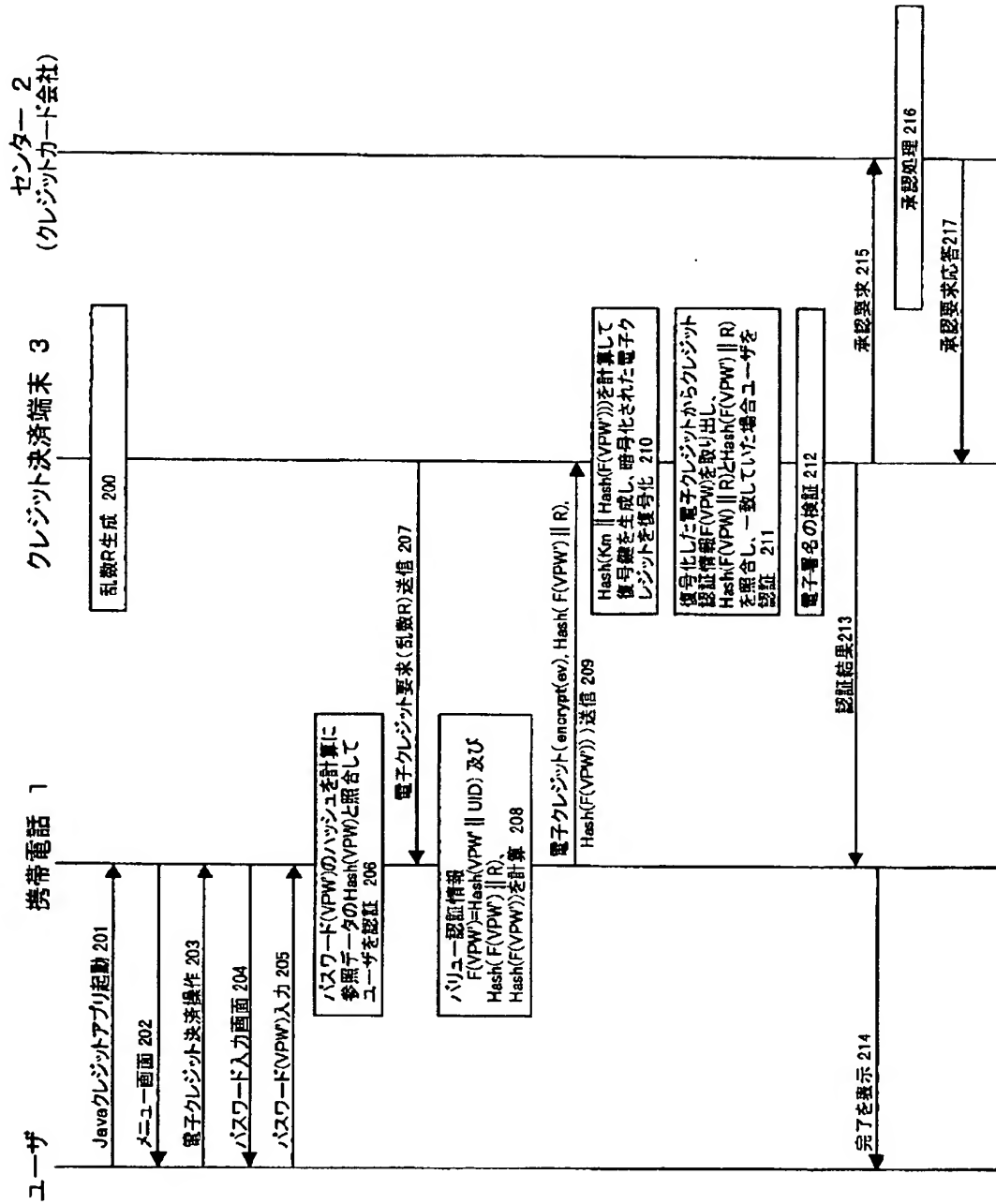
- 1 携帯電話
- 2 センター
- 3 クレジット決済端末

【書類名】 図面

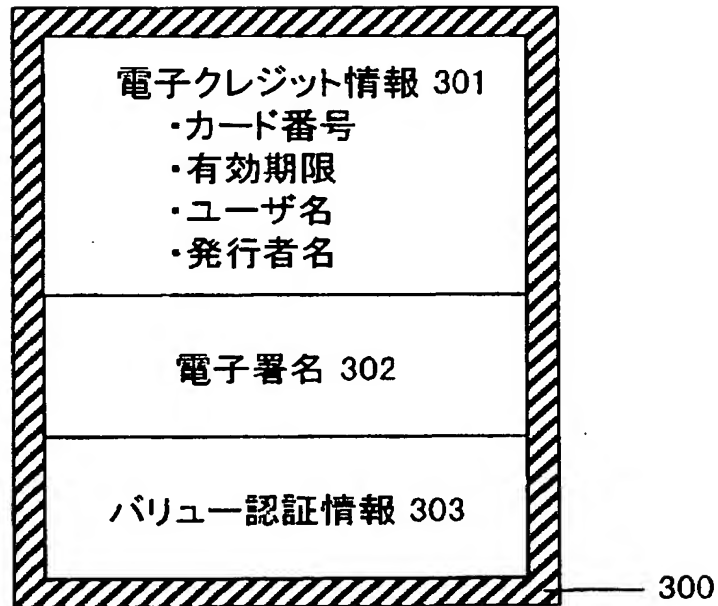
【図 1】



【図 2】



【図 3】



【書類名】 要約書

【要約】

【課題】 耐タンパ機能のない携帯端末であっても、電子バリュウの安全な認証処理が出来る認証システムを提供する。

【解決手段】 ユーザの携帯端末に暗号化された電子バリュウを格納し、電子バリュウにはユーザが指定した電子バリュウに対する認証情報(VPW)をハッシュ演算したバリュウ認証情報(F(VPW))が含まれており、ユーザを認証する処理において、認証装置が乱数Rを生成して携帯端末に送信し、携帯端末がユーザが入力した電子バリュウに対する認証情報(VPW')からバリュウ認証情報(F(VPW'))を生成し、更に、乱数Rと組み合わせたデータにハッシュ演算を行い認証情報Hash(F(VPW') || R)を生成して、暗号化された電子バリュウと共に認証装置に送信し、認証装置が受信した暗号化された電子バリュウの暗号を復号化して、電子バリュウからバリュウ認証情報(F(VPW))を取り出し、乱数Rと組み合わせたデータにハッシュ演算を行い認証情報Hash(F(VPW) || R)を生成し、受信した認証情報Hash(F(VPW') || R)と認証情報Hash(F(VPW) || R)とが一致することを検証して、ユーザを認証する。

【選択図】 図 2

特願 2 0 0 2 - 2 4 5 9 9 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社